

TABLE OF CONTENTS

Unit No.	Title	Page No.
	Part I: Foundations of IoT and Security	
1	Introduction to the Internet of Things	01-16
	1.1 Evolution of IoT	
	1.2 IoT Architecture and Communication Models	
	1.3 IoT Enabling Technologies	
	1.4 IoT Applications Across Domains	
	1.5 Security Challenges Unique to IoT	
2	Fundamentals of Cybersecurity	17-31
	2.1 Principles of Information Security (CIA Triad)	
	2.2 Threats, Vulnerabilities, and Attacks	
	2.3 Security Models and Trust Concepts	
	2.4 Risk Assessment and Security Metrics	
	2.5 Security Lifecycle Management	
	Part II: IoT Threat Landscape and Attack Models	
3	IoT Threat Modeling	32-46
	3.1 Adversary Models in IoT	
	3.2 Attack Surfaces in IoT Systems	
	3.3 STRIDE and DREAD Models for IoT	
	3.4 Kill Chain and Attack Lifecycle	
	3.5 Case Studies of Real-World IoT Attacks	
4	Network and Communication Attacks	47-60
	4.1 Eavesdropping and Traffic Analysis	
	4.2 Man-in-the-Middle Attacks	
	4.3 Denial-of-Service and DDoS Attacks	
	4.4 Routing and Sybil Attacks	
	4.5 Wireless-Specific Attacks	
	Part III: Cryptography and Secure Communication	
5	Lightweight Cryptography for IoT	61-74
	5.1 Constraints of IoT Devices	
	5.2 Lightweight Symmetric Cryptography	
	5.3 Lightweight Asymmetric Cryptography	
	5.4 Hash Functions and MACs	
	5.5 Performance and Energy Trade-offs	

6	Secure Communication Protocols	75-88
	6.1 TLS, DTLS, and OSCORE	
	6.2 Secure MQTT, CoAP, and AMQP	
	6.3 Key Management and Distribution	
	6.4 Secure Bootstrapping Mechanisms	
	6.5 Protocol-Level Vulnerabilities	
	Part IV: Device, Platform, and Data Security	
7	IoT Device and Hardware Security	89-103
	7.1 Secure Boot and Firmware Protection	
	7.2 Trusted Execution Environments	
	7.3 Physical Attacks and Countermeasures	
	7.4 Side-Channel Attacks	
	7.5 Hardware Security Modules (HSMs)	
8	Platform and Cloud Security	104-118
	8.1 IoT Middleware Security	
	8.2 Cloud-IoT Integration Risks	
	8.3 Identity and Access Management	
	8.4 Secure APIs and Microservices	
	8.5 Multi-Tenant Security Issues	
9	Data Security and Privacy	119-134
	9.1 Data Confidentiality and Integrity	
	9.2 Secure Data Storage and Processing	
	9.3 Privacy-Preserving Techniques	
	9.4 Data Anonymization and Encryption	
	9.5 Regulatory Compliance (GDPR, HIPAA, etc.)	
	Part V: Authentication, Authorization, and Trust	
10	Authentication Mechanisms	135-148
	10.1 Device and User Authentication	
	10.2 Certificate-Based Authentication	
	10.3 Biometric and Context-Aware Authentication	
	10.4 Mutual Authentication Protocols	
	10.5 Zero-Trust Architecture for IoT	
11	Authorization and Access Control	149-163
	11.1 Role-Based Access Control (RBAC)	
	11.2 Attribute-Based Access Control (ABAC)	
	11.3 Capability-Based Access Control	

	11.4	Policy Enforcement Mechanisms	
	11.5	Trust and Reputation Systems	
		Part VI: AI, Blockchain, and Emerging Security Technologies	
12		AI and Machine Learning for IoT Security	164-178
	12.1	Intrusion Detection Systems	
	12.2	Anomaly and Behavior-Based Detection	
	12.3	Federated Learning for IoT Security	
	12.4	Adversarial ML Attacks	
	12.5	Explainable AI in Security	
13		Blockchain and Distributed Ledger Security	179-193
	13.1	Blockchain Fundamentals for IoT	
	13.2	Secure Identity Management	
	13.3	Decentralized Trust Models	
	13.4	Smart Contracts for IoT Security	
	13.5	Scalability and Energy Challenges	
		Part VII: Domain-Specific IoT Security	
14		Industrial, Healthcare, and Smart Infrastructure Security	194-209
	14.1	Industrial IoT (IIoT) Security	
	14.2	Healthcare IoT and Medical Devices	
	14.3	Smart Grid and Energy Systems	
	14.4	Smart Cities and Transportation	
	14.5	Case Studies and Best Practices	
		Part VIII: Future Trends, Challenges, and Research Directions	
15		Future of IoT Security	210-224
	15.1	Post-Quantum Cryptography for IoT	
	15.2	Security in 6G and Massive IoT	
	15.3	Autonomous and Self-Healing Security Systems	
	15.4	Standardization and Global Policies	
	15.5	Open Research Challenges and Vision	
		Glossary of Terms	225
		Appendix A: IoT Security Standards and Frameworks	226
		Appendix B: Cryptographic Algorithms and Parameters	227
		Appendix C: Sample Security Architectures	228
		References	229
		Index	231